

Office of the Secretary of Defense

§ 310.8

(4) Ensure Component compliance with supplemental guidance and procedures in accordance with all applicable federal laws, regulations, policies, and procedures.

(5) Appoint a Component senior official for privacy (CSOP) to support the SAOP in carrying out the SAOP's duties identified in OMB Memorandum M-05-08.

(6) Appoint a Component privacy officer to administer the DoD Privacy Program, on behalf of the CSOP.

(7) Ensure DoD personnel and DoD contractors having primary responsibility for implementing the DoD Privacy Program receive appropriate privacy training. This training must be consistent with the requirements of this part and will address the provisions of 5 U.S.C. 552a, OMB Circular No. A-130, and this part.

(8) Ensure that all DoD Component legislative, regulatory, or other policy proposals are evaluated to ensure consistency with the information privacy requirements of this part.

(9) Assess the impact of technology on the privacy of PII and, when feasible, adopt privacy-enhancing technology to:

(i) Preserve and protect PII contained in a DoD Component system of records.

(ii) Audit compliance with the requirements of this part.

(10) Ensure that officials who have specialized knowledge of the DoD Privacy Program periodically review Component implementation of and compliance with the DoD Privacy Program.

(11) Submit reports, consistent with the requirements of this part, in accordance with 5 U.S.C. 552a and OMB Circular No. A-130, and as otherwise directed by the Chief, DPCLD.

(e) In addition to the responsibilities in paragraph (d), the Secretaries of the Military Departments provide program and financial support to the Combatant Commands as identified in DoD Directive 5100.03, "Support to the Headquarters of Combatant and Subordinate Unified Commands" (available at <http://www.dtic.mil/whs/directives/correspdf/510003p.pdf>) to fund, without reimbursement, the administrative and logistic support required by combatant and subordinate unified command

headquarters to perform their assigned missions effectively.

[80 FR 4209, Jan. 27, 2015]

§ 310.7 [Reserved]

§ 310.8 Rules of conduct.

In accordance with section (e)(9) of The Privacy Act, this section provides DoD rules of conduct for the development, operation, and maintenance of systems of records. DoD personnel and DoD contractor personnel will:

(a) Take action to ensure that any PII contained in a system of records that they access and use to conduct official business will be protected so that the security and confidentiality of the information is preserved.

(b) Not disclose any PII contained in any system of records, except as authorized by The Privacy Act, or other applicable statute, Executive order, regulation, or policy. Those willfully making any unlawful or unauthorized disclosure, knowing that disclosure is prohibited, may be subject to criminal penalties and/or administrative sanctions.

(c) Report any unauthorized disclosures of PII from a system of records to the applicable Privacy point of contact (POC) for the respective DoD Component.

(d) Report the maintenance of any system of records not authorized by this part to the applicable Privacy POC for the respective DoD Component.

(e) Minimize the collection of PII to that which is relevant and necessary to accomplish a purpose of the DoD.

(f) Not maintain records describing how any individual exercises rights guaranteed by the First Amendment, except:

(1) When specifically authorized by statute.

(2) When expressly authorized by the individual that the record is about.

(3) When the record is pertinent to and within the scope of an authorized law enforcement activity, including authorized intelligence or administrative activities.

(g) Safeguard the privacy of all individuals and the confidentiality of all PII.

(h) Limit the availability of records containing PII to DoD personnel and